UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,327	09/02/2003	Chih-Wei Chen	LA-7196-125	2925

167 7590 05/15/2007
FULBRIGHT AND JAWORSKI LLP
555 S. FLOWER STREET, 41ST FLOOR
LOS ANGELES, CA 90071

EXAMINER	
SIKRI, ANISH	
ART UNIT	PAPER NUMBER
2109	
MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/653,327	CHEN, CHIH-WEI	
	Examiner	Art Unit	
	Anish Sikri	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 September 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1 to 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hasan et al (US Pat 7,082,464) in view of Still (US Pat 5,991,879).

Consider **Claim 1**, Hasan et al discloses a network-linked computer platform configuration data access management method for use on a network-linked computer platform that is provided with at least one management function and linked to a network system linked to a number of system administration workstations (Hasan et al, Col 3 Lines 58-65, Col 4 Lines 9-13, Fig 1), for the purpose of allowing a group of system administrators to browse the configuration data of each management function of the network-linked computer platform (Hasan et al, Col 5 Lines 65-67, Col 6 Lines 1-7) at the same time while allowing only one system administrator to modify the configuration data of the same management function at the same time (Hasan et al, Col 16 Lines 38-43); the network-linked computer platform configuration data access management method comprising: establishing a table data module, which is a data-only module used to store the current-access-status property of each management function of the network-linked computer platform (Hasan et al, Col 16 Lines 49-54); in the event of any one of the system administration workstations issues a management function access request, inquiring the table data module whether the management function being requested for modification is currently being accessed (Hasan et al, Col 16 Lines 38-54).

But Hasan et al fails to disclose clearly if NO, generating an access-permit message; whereas if YES, generating an access-inhibit message; in response to the access-permit message, performing an access-status registration procedure to set the current-access-status property of the requested management function to TRUE in the table data module; and then permitting the requesting workstation to gain access to and modify the configuration data of the requested management function; and in response to the access-inhibit message, performing an access-inhibiting procedure to inhibit the requesting workstation to modify the configuration data of the requested management function.

Nonetheless, Still discloses if NO, generating an access-permit message; whereas if YES, generating an access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44); in response to the access-permit message, performing an access-status registration procedure to set the current-access-status property of the requested management function to TRUE in the table data module (Still, Col 5 Lines 48-65, Col 6 Lines 39-44); and then permitting the requesting workstation to gain access to and modify the configuration data of the requested management function (Still, Col 5 Lines 48-65, Col 6 Lines 39-44); and in response to the access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44), performing an access-inhibiting procedure to inhibit the requesting workstation to modify the configuration data of the requested management function (Still, Col 5 Lines 48-65, Col 6 Lines 39-44). Still's invention clearly shows when an object profile in a database is locked, and how the computer platform will incorporate access-permit message or access-inhibit message to the security administrator. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement the security steps taught by Still in the computer platform, taught by Hasan et al, for the purpose of preventing conflicting access to configuration objects of the database.

Consider **Claim 2**, and as applied to claim 1 above, Hasan et al as modified by Still fails to disclose a timing procedure, which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management function, and which is further capable of generating an access-inhibit message at timeout to inhibit access to the configuration data of the requested management function. Nonetheless, Still's invention clearly discloses a timing procedure (Still, Col 7 Lines 46-66), which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management function (Still, Col 7 Lines 46-66), and which is further capable of generating an access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) at timeout to inhibit access to the configuration data of the requested management function (Still, Col 7 Lines 46-66). Still's invention clearly shows on how grace periods can be incorporated into the computer platform when it comes to users/system users accessing data. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement timeout procedure of Still in a computer platform, of Hasan et al for the purpose of enabling grace timeouts which is able to lock (access-inhibit) the data after some pre-determined time access from the users/system users.

Consider **Claim 3**, and as applied to claim 1 above, Hasan et al as modified by Still fails to disclose the management function configuration data includes authorized user profiles, hard disk settings, and system security settings. Nonetheless, Still clearly discloses the management function configuration data includes authorized user profiles, hard disk settings, and system security settings (Still, Col 2 Lines 16-25, Lines 35-36, Col 4 Lines 13-15). Still's invention clearly shows a facet of system security files, which are used on a computer platform. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement the security/configuration/profile steps taught by Still in the computer platform taught by Hasan et al, for the purpose of configuring the system(s).

Consider **Claim 4**, and as applied to claim 1 above, Hasan et al as modified by Still clearly discloses the access-inhibiting procedure allows the system administrator at the requesting workstation to view the contents of the configuration data of the requested management function but not to modify (Hasan et al, Col 16 Lines 49-54). Hasan et al clearly shows on how the access control scheme can allow the administrator to have no access, read access only, or read and write access to any specific part of the management database.

Consider **Claim 5,** Hasan et al as modified by Still clearly network-linked computer platform configuration data access management system for use with a network-linked computer platform that is provided with at least one management function and linked to a network system linked to a number of system administration workstations (Hasan et al, Col 3 Lines 58-65, Col 4 Lines 9-13, Fig 1), for the purpose of allowing a group of system administrators to browse the configuration data of each management function of the network-linked computer platform (Hasan et al, Col 5 Lines 65-67, Col 6 Lines 1-7) at the same time while allowing only one system administrator to modify the configuration data of the same management function at the same time (Hasan et al, Col 16 Lines 38-43); the network-linked computer platform configuration data access management system comprising: a table data module, which is a data-only module used to store the current-access-status property of each management function of the network-linked computer platform (Hasan et al, Col 16 Lines 49-54); a request responding module, which is capable of detecting whether any one of the system administration workstations has issued a management function access request (Hasan et al, Col 16 Lines 38-54).

But Hasan et al fails to disclose and capable of issuing an inquiry request message; an inquiry module, which is capable of being activated in response to the inquiry request message from the request responding module to inquire the table data module whether the management function being requested for modification is currently being accessed; if NO, the inquiry module generating an access-permit message; whereas if YES, the inquiry module issuing an access-inhibit message; an access-status registration module, which is capable of being activated in response to the access-permit message from the inquiry module to set the current-access-status property of the requested management function to TRUE; and an access module, which is capable of being activated in response to the access-permit message from the inquiry module to allow the system administrator at the requesting workstation to gain access to and modify the configuration data of the requested management function, and capable of being activated in response to the access-inhibit message from the inquiry module to inhibit the system administrator at the requesting workstation to modify the configuration data of the management function.

Nonetheless, Still clearly discloses capable of issuing an inquiry request message; an inquiry module, which is capable of being activated in response to the inquiry request message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) from the request responding module to inquire the table data module whether the management function being requested for modification is currently being accessed; if NO, the inquiry module generating an access-permit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44); whereas if YES, the inquiry module issuing an access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44); an access-status registration module, which is capable of being activated in response to the access-permit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) from the inquiry module to set the current-access-status property of the requested management function to TRUE; and an access module, which is capable of being activated in response to the access-permit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) from the inquiry module to allow the system administrator at the requesting workstation to gain access to and modify the configuration data of the requested management function (Still, Col 5 Lines 48-65, Col 6 Lines 39-44), and capable of being activated in response to the access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) from the inquiry module to inhibit the system administrator at the requesting workstation to modify the configuration data of the management function (Still, Col 5 Lines 48-65, Col 6 Lines 39-44). Still's invention clearly shows when an object profile in a database is locked, and how the computer platform will incorporate access-permit message or access-inhibit message to the security administrator. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement the security steps taught by Still in the computer platform, taught by Hasan et al, for the purpose of preventing conflicting access to configuration objects of the database.

Consider **Claim 6**, and as applied to claim 5 above, Hasan et al as modified by Still clearly fails to disclose a timing module, which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management function, and which is further capable of generating an access-inhibit message at timeout to inhibit access to the configuration data of the requested management function. Nonetheless, Still clearly discloses a timing module (Still, Col 7 Lines 46-66), which is capable of being activated to count time for a preset timeout length promptly after the system administrator at the requesting workstation starts modifying the configuration data of the requested management function (Still, Col 7

Lines 46-66), and which is further capable of generating an access-inhibit message (Still, Col 5 Lines 48-65, Col 6 Lines 39-44) at timeout to inhibit access to the configuration data of the requested management function (Still, Col 5 Lines 48-65, Col 6 Lines 39-44). Still's invention clearly shows on how grace periods can be incorporated into the computer platform when it comes to users/system users accessing data. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement timeout procedure of Still in a computer platform of Hasan et al for the purpose of enabling grace timeouts which is able to lock (access-inhibit) the data after some pre-determined time access from the users/system users.

Consider **Claim 7**, and as applied to claim 5 above, Hasan et al as modified by Still clearly fails to disclose the management function configuration data includes authorized user profiles, hard disk settings, and system security settings. Nonetheless, Still clearly discloses the management function configuration data includes authorized user profiles, hard disk settings, and system security settings (Still, Col 2 Lines 16-25, Lines 35-36, Col 4 Lines 13-15). Still's invention clearly shows a facet of system security files, which are used on a computer platform. Therefore, it would be obvious to a person of ordinary skill in the art at the time of the invention was made to implement the security/configuration/profile steps taught by Still in the computer platform taught by Hasan et al, for the purpose of configuring the system(s).

Consider **Claim 8**, and as applied to claim 5 above, Hasan et al as modified by Still clearly discloses the access module, when inhibited, allows the system administrator at the requesting workstation to view the contents of the configuration data of the requested management function but not to modify (Hasan et al, Col 16 Lines 49-54). Hasan et al clearly shows on how the access control scheme can allow the administrator to have no access, read access only, or read and write access to any specific part of the management database.

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Anish Sikri whose telephone number is (571) 270-1783. The Examiner can normally be reached on Monday-Thursday from 6:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Rafael Pérez-Gutiérrez can be reached on (571) 272-7915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Anish Sikri
A.S./as

May 8, 2007

RAFAEL PEREZ-GUTIERREZ
SUPERVISORY PATENT EXAMINER
5/10/07